

**Notice of Allowability**

Application No.

09/717,761

Examiner

Tongoc Tran

Applicant(s)

QIU ET AL.

Art Unit

2134

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 3/15/2005.
2. ☒ The allowed claim(s) is/are 1-48.
3. ☒ The drawings filed on 15 March 2005 are accepted by the Examiner.
4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☐ All   b) ☐ Some\*   c) ☐ None   of the:
    1. ☐ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).
  - \* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6. ☐ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit  
of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413),  
Paper No./Mail Date \_\_\_\_\_
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

PD

### **DETAILED ACTION**

1. This office action is in response to Applicant's amendment filed on 3/15/2005. Claims 1, 11, 20, 21, 25, 40 and 48 have been amended. Claims 5 and 29 have been cancelled. Claims 1-4, 6-28 and 30-48 are pending.

### ***Allowable Subject Matter***

2. Claims 1-4, 6-28 and 30-48 are allowed.

The following is an examiner's statement of reasons for allowance:

The present invention is directed to method and system for providing a non-linear keystream generation algorithm using a combination of static (or linear) feedback shift registers and dynamic (or non-linear) feedback shift registers. The system is an improvement of the commonly assigned U.S. Patent, Brown, Patent No. 4,860,353, describes a dynamic feedback arrangement scrambling technique (DFAST) keystream generator, refers to as DFAST2. The cited prior art, Brown, fails to disclose a plurality of dynamic feedback shift registers and at least one static feedback shift registers and providing data bits from predetermined register stages of each shift register to randomization stages which permute the data bits to generate a stronger keystream which Applicants claim to be the unique features of the newly improved DFAST2. The art of record, Stoklosa, teaches using hash functions to compute integrity of data which by providing multiplexer and shift registers generating maximum length sequence. One implementation is built with the help of some nonlinear feedback shift registers, one linear feedback shift register and

Art Unit: 2134

one multiplexer. The second cited prior art, Schneier, discloses stream ciphers can rely on confusion and diffusion techniques through substitution or permutation in order to obscure or dissipates the redundancy of plaintext message. Schneier however, does not explicitly disclose the permutation is implemented by permutating data bits at a plurality of randomization stages where the data bits are received from predetermined registers stages of a plurality of dynamic feedback shift registers and at least one feedback shift register as claimed and presented by Applicants in the remark. Therefore, in view of the amendment and Applicants' remark, the art of record either singularly or in combination, fails to anticipate or render the claimed features obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### ***Conclusion***

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (571) 272-3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Art Unit: 2134

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran  
Art Unit: 2134

TT

 May 24, 2005

  
GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER